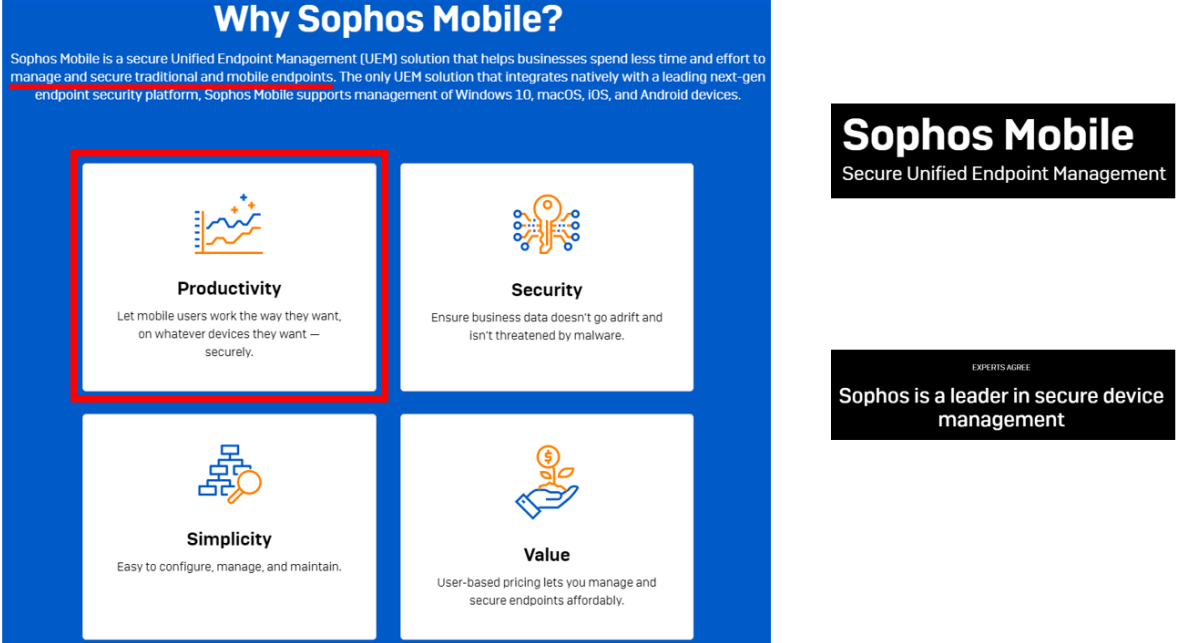


Exhibit 8

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.


Exhibit 8 – U.S. Patent No. 9,147,085

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
<p>[1pre] A method of establishing plural modes of operation on a mobile device, the method comprising:</p>	<p>Sophos Mobile is an endpoint (e.g., mobile device) management tool</p>  <p>https://www.sophos.com/en-us/products/mobile-control</p>


Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Sophos Mobile supports BYOD environments through the management “mode” of Android (Android Enterprise Work Profile) to separate business and personal data. For example, corporate email and apps remain separate from personal data. It is possible to configure “policies” and establish “blacklist” and “whitelist” applications.</p> <div data-bbox="625 500 1780 1015">  <p>Sophos Mobile Means Enterprise Mobility Management Manage in Sophos Central</p> <div> <p>Devices</p> <ul style="list-style-type: none"> ✓ iOS, Android, Windows 10, macOS ✓ Configuration and policies ✓ Inventory and asset management ✓ Detailed reporting </div> <div> <p>Apps</p> <ul style="list-style-type: none"> ✓ Install, remove, and view apps ✓ Enterprise app store ✓ App control, whitelist/blacklist ✓ Manage and configure Office 365 apps </div> <div> <p>Flexible</p> <ul style="list-style-type: none"> ✓ Manage corporate devices ✓ Manage bring-your-own-device (BYOD) ✓ Secure business data ✓ Respect user privacy </div> <div> <p>Security</p> <ul style="list-style-type: none"> ✓ Extended Detection and Response ✓ Malware, ransomware, PUAs ✓ Anti-phishing ✓ Web protection, web filtering </div> <div> <p>Bring Your Own Device? No Problem!</p> <p>Sophos Mobile lets you secure any combination of personal and corporate-owned devices with minimal effort.</p> <p>Sophos Mobile supports BYOD environments through the Android Enterprise Work Profile and iOS User Enrollment modes of management, to ensure that business data is safe and personal information is private. Deploy corporate email and apps to a device and feel safe knowing these remain separate from a user's personal data, enabling productivity without compromising security.</p> </div> </div> <p>https://www.sophos.com/en-us/products/mobile-control</p>

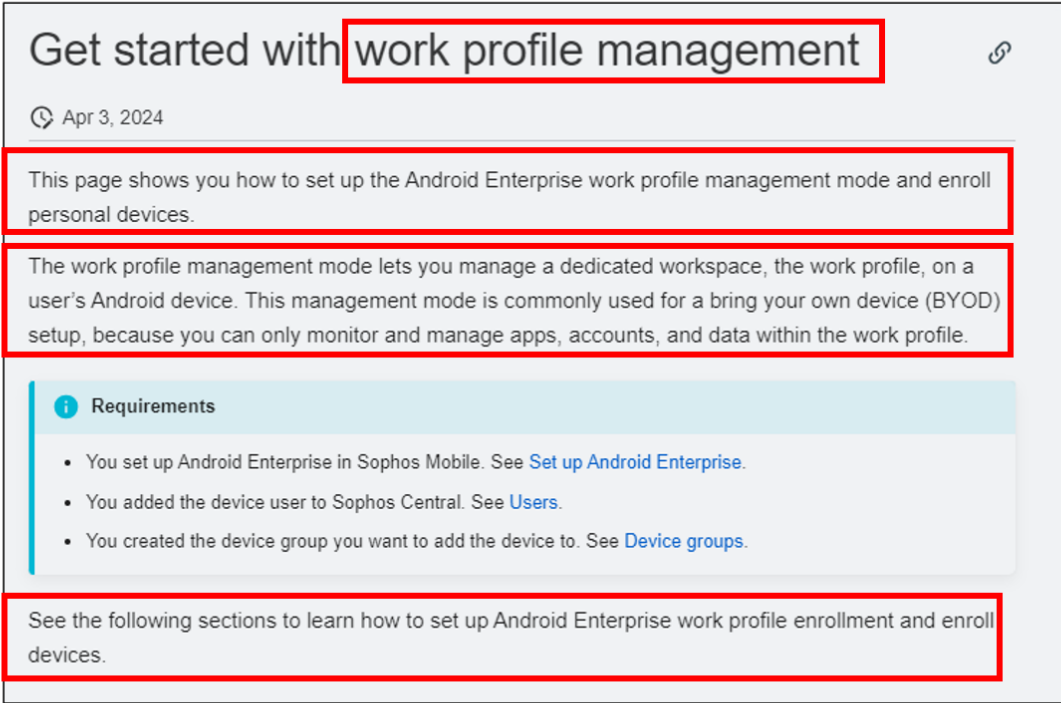
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
<p>[1a] associating each application on the mobile device with one of a plurality of modes; and</p>	<p>Sophos Mobile supports the use of Android Enterprise Work Profile mode.</p> <div data-bbox="667 462 1875 976">  <h2 data-bbox="1209 540 1791 646">Bring Your Own Device? No Problem!</h2> <p data-bbox="1209 672 1770 719">Sophos Mobile lets you secure any combination of personal and corporate-owned devices with minimal effort.</p> <p data-bbox="1209 742 1860 816">Sophos Mobile supports BYOD environments through the Android Enterprise Work Profile and iOS User Enrolment modes of management to ensure that business data is safe and personal information is private.</p> <p data-bbox="1209 821 1854 896">Deploy corporate email and apps to a device and feel safe knowing these remain separate from a user's personal data, enabling productivity without compromising security.</p> </div> <p data-bbox="1060 1143 1829 1175">https://www.sophos.com/en-us/products/mobile-control</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p data-bbox="611 318 1493 345">Sophos Mobile supports the use of Android Enterprise Work Profile mode.</p> <div data-bbox="739 402 1793 1101">  <p data-bbox="766 428 1598 472">Get started with work profile management</p> <p data-bbox="766 505 903 529">Apr 3, 2024</p> <p data-bbox="766 570 1724 626">This page shows you how to set up the Android Enterprise work profile management mode and enroll personal devices.</p> <p data-bbox="766 654 1734 743">The work profile management mode lets you manage a dedicated workspace, the work profile, on a user's Android device. This management mode is commonly used for a bring your own device (BYOD) setup, because you can only monitor and manage apps, accounts, and data within the work profile.</p> <p data-bbox="793 792 953 816">Requirements</p> <ul data-bbox="800 849 1482 951" style="list-style-type: none"> • You set up Android Enterprise in Sophos Mobile. See Set up Android Enterprise. • You added the device user to Sophos Central. See Users. • You created the device group you want to add the device to. See Device groups. <p data-bbox="766 1008 1724 1065">See the following sections to learn how to set up Android Enterprise work profile enrollment and enroll devices.</p> </div> <p data-bbox="611 1170 1860 1195">https://docs.sophos.com/central/Mobile/help/en-us/AdminHelp/EnrollDevices/AndroidEnterprise/WorkProfileGetStarted/index.html</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p data-bbox="617 321 1801 383">Sophos Mobile supports the use of Android Enterprise Work Profile mode, which separates “work” and “personal” apps and data.</p> <div data-bbox="640 472 1862 771"> </div> <div data-bbox="753 836 1719 1015"> <h3 data-bbox="795 857 1066 902">Work Profile</h3> <div data-bbox="795 922 1680 974" style="border: 1px solid red; padding: 5px;"> <p>Separate work apps and data (managed by your organization) from employee personal data on employee and company-owned devices.</p> </div> </div> <p data-bbox="884 1109 1566 1141">https://www.android.com/enterprise/work-profile/</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>In Android Enterprise Work Profile mode, “work” apps and data are associated with a work profile as separate from and “personal” apps and data.</p> <div><h3>Work Profile and its features</h3><p>A Work Profile is a self contained profile on an Android device for storing work apps and data. Work Profile allows separation of work apps and data, giving organizations full control of the data, apps, and security policies within a Work Profile. Simultaneously, users retain privacy over their personal apps, data, and usage. On devices designated as company-owned during setup, organizations can enforce some policies that apply to a device’s personal profile and overall device behavior.</p><p>Apps installed in the Work Profile are marked with the briefcase icon, so as to be easily distinguishable from personal apps. For more information on how to use a Work Profile device, see What is a Work Profile.</p></div> <p>https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>

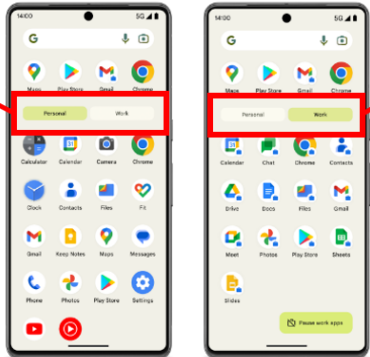
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification										
	<p data-bbox="617 321 1860 381">In Android Enterprise Work Profile mode, “work” apps and data are associated with a work profile as separate from and “personal” apps and data.</p> <div data-bbox="709 475 1766 1036" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p data-bbox="718 483 968 516">App management</p> <p data-bbox="718 537 1709 634">EMM providers support Android app management through an enterprise version of Google Play, called managed Google Play. With an EMM, you can create Managed Google Play accounts* for your users. These accounts enable app distribution to their Work Profiles.</p> <table data-bbox="718 659 1724 946"> <thead> <tr> <th data-bbox="718 659 1047 695">Feature</th><th data-bbox="1047 659 1724 695">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="718 695 1047 776">View and manage your app catalog</td><td data-bbox="1047 695 1724 776">View a list of purchased apps, approved apps, and private apps.</td></tr> <tr> <td data-bbox="718 776 1047 821">Distribute apps silently</td><td data-bbox="1047 776 1724 821">Silently install apps on a device without any user interaction.</td></tr> <tr> <td data-bbox="718 821 1047 902">Download apps from the managed Play app</td><td data-bbox="1047 821 1724 902">Users can install and update apps approved for them through the Managed Google Play app on their device.</td></tr> <tr> <td data-bbox="718 902 1047 946">Set managed configurations</td><td data-bbox="1047 902 1724 946">Configure work apps for individual users or devices.</td></tr> </tbody> </table> <p data-bbox="718 967 1692 1024">*For organizations with Google Workspace or Cloud Identity, users can access managed Google Play with their Google Workspace or Cloud Identity account.</p> </div> <p data-bbox="617 1097 1692 1166">https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>	Feature	Description	View and manage your app catalog	View a list of purchased apps, approved apps, and private apps.	Distribute apps silently	Silently install apps on a device without any user interaction.	Download apps from the managed Play app	Users can install and update apps approved for them through the Managed Google Play app on their device.	Set managed configurations	Configure work apps for individual users or devices.
Feature	Description										
View and manage your app catalog	View a list of purchased apps, approved apps, and private apps.										
Distribute apps silently	Silently install apps on a device without any user interaction.										
Download apps from the managed Play app	Users can install and update apps approved for them through the Managed Google Play app on their device.										
Set managed configurations	Configure work apps for individual users or devices.										

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p data-bbox="619 289 1871 349">In Android Enterprise Work Profile mode, “work” apps and data are associated with a work profile as separate from and “personal” apps and data.</p> <div data-bbox="611 370 1856 1101"> <p data-bbox="976 386 1423 418">What is an Android Work Profile?</p> <p data-bbox="976 430 1192 451"><i>Android 5 or later devices only</i></p> <div data-bbox="976 462 1640 560" style="border: 2px solid red; padding: 5px;"> <p data-bbox="976 462 1640 560">An Android Work Profile can be set up on an Android device to separate work apps and data from personal apps and data. With a Work Profile you can securely and privately use the same device for work and personal purposes—your organization manages your work apps and data while your personal apps, data, and usage remain private.</p> </div> <p data-bbox="995 581 1575 602">Note: Work Profile apps can't access SMS/MMS data from the personal profile on Android 11+.</p> <p data-bbox="976 630 1640 673">If your organization supports enrolling devices to use a Work Profile, your IT department should provide instructions on how to add one to your device.</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div data-bbox="611 690 1010 776" style="border: 2px solid red; padding: 5px; text-align: center;"> <div style="background-color: #d4edda; padding: 2px 10px; border-radius: 10px;">Personal</div> <div style="background-color: #fff3cd; padding: 2px 10px; border-radius: 10px;">Work</div> </div> <div data-bbox="1031 738 1398 1092">  </div> <div data-bbox="1461 706 1856 781" style="border: 2px solid red; padding: 5px; text-align: center;"> <div style="background-color: #fff3cd; padding: 2px 10px; border-radius: 10px;">Personal</div> <div style="background-color: #d4edda; padding: 2px 10px; border-radius: 10px;">Work</div> </div> </div> </div> <p data-bbox="619 1122 1493 1154">https://support.google.com/work/android/answer/6191949?hl=en</p>


Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
<p>[1b] restricting data on the mobile device to be accessible by only a subset of applications based on the mode associated with the application,</p>	<p>Android Enterprise Work Profile enables the creation of “approved app lists” that restricts data accessed by applications based on the mode.</p> <div data-bbox="680 526 1862 922"> <h2>Highlights</h2> <ul style="list-style-type: none"> ✓ Unlock personal devices Allow employees to use personal Android devices for work with full management control over data in Work Profile only. ✓ Manage approved app lists Choose which apps your employees can access on the Work Profile without restricting apps they can access on their personal profile. ✓ Remotely provision devices Provision company-owned devices remotely with zero-touch enrollment and get employees up-and-running right out of the box. </div> <p>https://www.android.com/enterprise/work-profile/</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p data-bbox="615 321 1871 418">Android Enterprise Work Profile restricts data to be accessible based on the mode associated with the app, as apps are restricted to segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles.</p> <div data-bbox="701 496 1816 1101" style="border: 2px solid red; padding: 10px;"> <p data-bbox="737 516 982 548">Data segregation</p> <p data-bbox="737 573 1218 597">Work profiles use the following data segregation rules.</p> <p data-bbox="737 646 835 670">Apps </p> <p data-bbox="737 698 1801 784">When the same app exists in the primary user and work profile, apps are scoped with their own segregated data. Generally, apps act independently and can't communicate directly with instances across the profile-user boundary unless they hold <code>INTERACT_ACROSS_PROFILES</code> permission or App-ops.</p> <p data-bbox="737 829 842 854">Accounts</p> <p data-bbox="737 881 1785 938">Accounts in the work profile are unique from the primary user and credentials can't be accessed across the profile-user boundary. Only apps in their respective context are able to access their respective accounts.</p> <p data-bbox="737 984 814 1008">Intents</p> <p data-bbox="737 1036 1745 1092">The administrator controls whether intents are resolved in or out of the work profile. By default, apps from the work profile are scoped to stay within the work profile exception of the Device Policy API.</p> </div> <p data-bbox="718 1130 1593 1162">https://source.android.com/docs/devices/admin/managed-profiles</p>


Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p data-bbox="615 282 1877 342">Android Enterprise Work Profile enables the creation of “policies” that restrict data accessed by applications and control permissions based on the mode (e.g., “work” or “personal”) associated with the app.</p> <div data-bbox="707 544 1793 846"><p data-bbox="745 573 1709 678">What policies is my organization enforcing on my device?</p><p data-bbox="745 699 1751 833">If your device has a work profile, your organization can view and manage your work apps and data. Your personal apps, data, and usage details aren't visible or accessible to your organization. Your organization may be able to manage certain settings on your device (e.g. time and date, language, Wi-Fi configurations) if your device is company-owned.</p></div> <p data-bbox="615 1040 1663 1068">https://support.google.com/work/android/answer/7502354?sjid=4365723958134001885-NC</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p data-bbox="617 289 1871 350">Android Enterprise Work Profile enables the creation of “policies” that restrict data accessed by applications and control permissions based on the mode (e.g., “work” or “personal”) associated with the app.</p> <div data-bbox="648 620 1793 808"><p data-bbox="678 638 951 678">Work profile </p><p data-bbox="1635 651 1749 667">Send feedback</p><p data-bbox="678 716 1749 792">The work profile solution set is intended for employee-owned devices and company-owned devices for work and personal use. Corporate apps, data, and management policies are restricted to the work profile. With a work profile, the same device can be used securely and privately for work and personal purposes.</p></div> <p data-bbox="617 1049 1549 1081">https://developers.google.com/android/work/requirements/work-profile</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p data-bbox="615 285 1883 380">Android Enterprise Work Profile enables the creation of “policies” that restrict data accessed by applications and control permissions based on the mode (e.g., “work” or “personal”) associated with the app. Sophos Mobile provides a device policy controller app for implementing and managing Android Enterprise Work Profile.</p> <div data-bbox="804 420 1629 992" style="border: 2px solid red; padding: 10px;"> <p data-bbox="842 436 1442 459">What policies can my organization manage on my device?</p> <p data-bbox="842 477 1581 602">When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p> <p data-bbox="842 623 1539 670">If your device is personally-owned, your organization can carry out some or all of the following actions:</p> <ul data-bbox="842 690 1585 987" style="list-style-type: none"> • Remotely create, access, and delete data in your work profile • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • Restrict what can be shared across your work and personal profiles • Block screen captures in your work profile • Manage access to your organization’s corporate mail server and internal data • Remotely install (and uninstall) apps and certificates in your work profile • Manage permissions and other settings for apps in your work profile </div> <p data-bbox="615 1050 1806 1073">https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification																
	<p data-bbox="611 326 1883 386">Android Enterprise Work Profile enables the creation of “policies” that restrict data accessed by applications and control permissions based on the mode (e.g., “work” or “personal”) associated with the app.</p> <div data-bbox="741 448 1734 1089"> <p data-bbox="779 467 1041 496">Device management</p> <table data-bbox="779 513 1684 1065"> <thead> <tr> <th data-bbox="779 513 1058 548">Feature</th><th data-bbox="1058 513 1684 548">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="779 548 1058 621">Manage Google Workspace accounts</td><td data-bbox="1058 548 1684 621">Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.</td></tr> <tr> <td data-bbox="779 621 1058 719">Manage 3rd party certificates</td><td data-bbox="1058 621 1684 719">Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.</td></tr> <tr> <td data-bbox="779 719 1058 816">Control access to input methods</td><td data-bbox="1058 719 1684 816">Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles</td></tr> <tr> <td data-bbox="779 816 1058 889">Control access to accessibility services</td><td data-bbox="1058 816 1684 889">Configure the accessibility services that can be enabled on a device.</td></tr> <tr> <td data-bbox="779 889 1058 979">Set location sharing preferences</td><td data-bbox="1058 889 1684 979">Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.</td></tr> <tr> <td data-bbox="779 979 1058 1027">Disable screen captures</td><td data-bbox="1058 979 1684 1027">Prevent users from taking screenshots when using apps in a Work Profile.</td></tr> <tr> <td data-bbox="779 1027 1058 1065">Retrieve network statistics</td><td data-bbox="1058 1027 1684 1065">Retrieve network usage statistics for a Work Profile.</td></tr> </tbody> </table> </div> <p data-bbox="640 1146 1864 1170">https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>	Feature	Description	Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.	Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.	Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles	Control access to accessibility services	Configure the accessibility services that can be enabled on a device.	Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.	Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.	Retrieve network statistics	Retrieve network usage statistics for a Work Profile.
Feature	Description																
Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.																
Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.																
Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles																
Control access to accessibility services	Configure the accessibility services that can be enabled on a device.																
Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.																
Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.																
Retrieve network statistics	Retrieve network usage statistics for a Work Profile.																

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
<p>[1c] wherein the data is associated with one of the plurality of modes and the restricting comprises adding a group permission to the data and providing each application with access to the data based on the group permission, the group permission for data associated with one of the plurality of modes controls access to the data by applications associated with the others of the plurality of modes, and</p>	<p>Android Enterprise Work Profile segregates data and <u>associates</u> data with one of the plurality of modes (i.e., “work” or “personal”), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the “work” or “personal” mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the “work” or “personal” mode), where the group permission for “work” mode controls access to “work” data by “personal” apps.</p> <div data-bbox="745 557 1732 1089" style="border: 2px solid red; padding: 10px; margin: 10px 0;"> <p>Data segregation</p> <p>Work profiles use the following data segregation rules.</p> <p>Apps ↗</p> <p>When the same app exists in the primary user and work profile, apps are scoped with their own segregated data. Generally, apps act independently and can't communicate directly with instances across the profile-user boundary unless they hold INTERACT_ACROSS_PROFILES permission or App-ops.</p> <p>Accounts</p> <p>Accounts in the work profile are unique from the primary user and credentials can't be accessed across the profile-user boundary. Only apps in their respective context are able to access their respective accounts.</p> <p>Intents</p> <p>The administrator controls whether intents are resolved in or out of the work profile. By default, apps from the work profile are scoped to stay within the work profile exception of the Device Policy API.</p> </div> <p>https://source.android.com/docs/devices/admin/managed-profiles</p>


Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p data-bbox="611 318 1877 513">Android Enterprise Work Profile segregates data and <u>associates</u> data with one of the plurality of modes (i.e., “work” or “personal”), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the “work” or “personal” mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the “work” or “personal” mode), where the group permission for “work” mode controls access to “work” data by “personal” apps.</p> <div data-bbox="705 578 1793 883"><p data-bbox="743 610 1709 716">What policies is my organization enforcing on my device?</p><p data-bbox="743 737 1751 870">If your device has a <u>work profile</u>, your organization can view and manage your work apps and data. Your personal apps, data, and usage details aren't visible or accessible to your organization. Your organization may be able to manage certain settings on your device (e.g. time and date, language, Wi-Fi configurations) if your device is company-owned.</p></div> <p data-bbox="611 1078 1667 1105">https://support.google.com/work/android/answer/7502354?sjid=4365723958134001885-NC</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p data-bbox="611 321 1875 516">Android Enterprise Work Profile segregates data and <u>associates</u> data with one of the plurality of modes (i.e., “work” or “personal”), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the “work” or “personal” mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the “work” or “personal” mode), where the group permission for “work” mode controls access to “work” data by “personal” apps.</p> <div data-bbox="644 654 1797 844"><p data-bbox="674 672 947 711">Work profile </p><p data-bbox="1635 685 1751 701">Send feedback</p><p data-bbox="674 753 1751 828">The work profile solution set is intended for <u>employee-owned devices</u> and <u>company-owned devices for work and personal use</u>. Corporate apps, data, and management policies are restricted to the work profile. With a work profile, the same device can be used securely and privately for work and personal purposes.</p></div> <p data-bbox="611 1084 1549 1117">https://developers.google.com/android/work/requirements/work-profile</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p>Android Enterprise Work Profile segregates data and <u>associates</u> data with one of the plurality of modes (i.e., “work” or “personal”), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the “work” or “personal” mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the “work” or “personal” mode), where the group permission for “work” mode controls access to “work” data by “personal” apps.</p> <div data-bbox="800 561 1623 1133" style="border: 2px solid red; padding: 10px;"> <p>What policies can my organization manage on my device?</p> <p>When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p> <p>If your device is personally-owned, your organization can carry out some or all of the following actions:</p> <ul style="list-style-type: none"> • Remotely create, access, and delete data in your work profile • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • <u>Restrict what can be shared across your work and personal profiles</u> • Block screen captures in your work profile • <u>Manage access to your organization's corporate mail server and internal data</u> • Remotely install (and uninstall) apps and certificates in your work profile • Manage permissions and other settings for apps in your work profile </div> <p>https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification																
	<p data-bbox="611 321 1885 516">Android Enterprise Work Profile segregates data and <u>associates</u> data with one of the plurality of modes (i.e., “work” or “personal”), as apps are restricted to accessing their own segregated data (and can only cross profile boundaries with permission), even when the same app exists in both profiles. A group permission is added to the data (e.g., as part of associating data with the “work” or “personal” mode), and applications are provided access to the data based on the group permission (e.g., based on being associated with the “work” or “personal” mode), where the group permission for “work” mode controls access to “work” data by “personal” apps.</p> <div data-bbox="745 527 1732 1166"> <p data-bbox="785 548 1045 576">Device management</p> <table data-bbox="785 592 1684 1140"> <thead> <tr> <th data-bbox="785 592 1060 630">Feature</th><th data-bbox="1060 592 1684 630">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="785 630 1060 701">Manage Google Workspace accounts</td><td data-bbox="1060 630 1684 701">Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.</td></tr> <tr> <td data-bbox="785 701 1060 799">Manage 3rd party certificates</td><td data-bbox="1060 701 1684 799">Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.</td></tr> <tr> <td data-bbox="785 799 1060 896">Control access to input methods</td><td data-bbox="1060 799 1684 896">Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles</td></tr> <tr> <td data-bbox="785 896 1060 961">Control access to accessibility services</td><td data-bbox="1060 896 1684 961">Configure the accessibility services that can be enabled on a device.</td></tr> <tr> <td data-bbox="785 961 1060 1026">Set location sharing preferences</td><td data-bbox="1060 961 1684 1026">Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.</td></tr> <tr> <td data-bbox="785 1026 1060 1091">Disable screen captures</td><td data-bbox="1060 1026 1684 1091">Prevent users from taking screenshots when using apps in a Work Profile.</td></tr> <tr> <td data-bbox="785 1091 1060 1140">Retrieve network statistics</td><td data-bbox="1060 1091 1684 1140">Retrieve network usage statistics for a Work Profile.</td></tr> </tbody> </table> </div> <p data-bbox="638 1170 1869 1193">https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features</p>	Feature	Description	Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.	Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.	Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles	Control access to accessibility services	Configure the accessibility services that can be enabled on a device.	Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.	Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.	Retrieve network statistics	Retrieve network usage statistics for a Work Profile.
Feature	Description																
Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.																
Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.																
Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles																
Control access to accessibility services	Configure the accessibility services that can be enabled on a device.																
Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.																
Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.																
Retrieve network statistics	Retrieve network usage statistics for a Work Profile.																

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
<p>[1d] the group permission for the data limits the ability to copy a subset of the data between modes, where some data can be copied directly between modes, and</p>	<p>Android Enterprise Work Profile polices can limit the ability to copy data between modes.</p> <div data-bbox="816 470 1686 1070" style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"> <p>What policies can my organization manage on my device?</p> <p>When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p> <p>If your device is personally-owned, your organization can carry out some or all of the following actions:</p> <ul style="list-style-type: none"> • Remotely create, access, and delete data in your work profile • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • Restrict what can be shared across your work and personal profiles • Block screen captures in your work profile • Manage access to your organization's corporate mail server and internal data • Remotely install (and uninstall) apps and certificates in your work profile • Manage permissions and other settings for apps in your work profile </div> <p>https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>


Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification																
	<p data-bbox="617 326 1625 354">Android Enterprise Work Profile polices can limit the ability to copy data between modes.</p> <div data-bbox="743 444 1740 1089"> <p data-bbox="785 467 1045 495">Device management</p> <table border="1"> <thead> <tr> <th data-bbox="785 511 1066 548">Feature</th><th data-bbox="1066 511 1690 548">Description</th></tr> </thead> <tbody> <tr> <td data-bbox="785 557 1066 618">Manage Google Workspace accounts</td><td data-bbox="1066 557 1690 618">Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.</td></tr> <tr> <td data-bbox="785 626 1066 711">Manage 3rd party certificates</td><td data-bbox="1066 626 1690 711">Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.</td></tr> <tr> <td data-bbox="785 719 1066 820">Control access to input methods</td><td data-bbox="1066 719 1690 820">Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles</td></tr> <tr> <td data-bbox="785 828 1066 889">Control access to accessibility services</td><td data-bbox="1066 828 1690 889">Configure the accessibility services that can be enabled on a device.</td></tr> <tr> <td data-bbox="785 898 1066 959">Set location sharing preferences</td><td data-bbox="1066 898 1690 959">Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.</td></tr> <tr> <td data-bbox="785 967 1066 1029">Disable screen captures</td><td data-bbox="1066 967 1690 1029">Prevent users from taking screenshots when using apps in a Work Profile.</td></tr> <tr> <td data-bbox="785 1037 1066 1065">Retrieve network statistics</td><td data-bbox="1066 1037 1690 1065">Retrieve network usage statistics for a Work Profile.</td></tr> </tbody> </table> </div> <p data-bbox="644 1146 1871 1170"> https://support.google.com/work/android/answer/9563584?hl=en#zippy=%2Ckey-features%2Cadvanced-features%2Cadditional-features </p>	Feature	Description	Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.	Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.	Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles	Control access to accessibility services	Configure the accessibility services that can be enabled on a device.	Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.	Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.	Retrieve network statistics	Retrieve network usage statistics for a Work Profile.
Feature	Description																
Manage Google Workspace accounts	Ensure that only authorized Google Workspace (or Cloud Identity) accounts can interact with corporate data.																
Manage 3rd party certificates	Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore.																
Control access to input methods	Configure the input methods (e.g. keyboards) that a user can configure on their device. Input methods are shared across both work and personal profiles																
Control access to accessibility services	Configure the accessibility services that can be enabled on a device.																
Set location sharing preferences	Configure location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps in a Work Profile.																
Disable screen captures	Prevent users from taking screenshots when using apps in a Work Profile.																
Retrieve network statistics	Retrieve network usage statistics for a Work Profile.																

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
<p>[1e] wherein data associated with the first mode is deleted from the mobile device when such data is not accessed within a time period, while data associated with the second mode does not have a deletion policy.</p>	<p>Android Enterprise Work Profile allows work profile administrator to control the “lifetime” and “egress” of data.</p> <div data-bbox="768 537 1791 1005"> <h3>Employing Work Profiles </h3> <p>A <i>work profile</i> is a managed profile that has separate app data from the primary user profile but shares some system-wide settings, such as Wi-Fi and Bluetooth. The primary goal of a work profile is to create a segregated and secure container to hold managed data. <u>The administrator of a work profile has full control over the scope, ingress, egress, and lifetime of data.</u> Following are some characteristics of work profiles:</p> <ul style="list-style-type: none"> • Creation. Any app in the primary user can create a work profile. The user is notified of work profile behaviors and policy enforcement before creation. • Management. Apps known as <i>profile owners</i> can programmatically invoke APIs in the DevicePolicyManager class to restrict use. Profile owners are defined at initial profile setup. Policies unique to work profiles involve app restrictions, updatability, and intent behaviors. • Visual treatment. Apps, notifications, and widgets from the work profile are badged and typically made available inline with user interface (UI) elements from the primary user. </div> <p>https://source.android.com/docs/devices/admin/managed-profiles</p>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.

Exhibit 8 – U.S. Patent No. 9,147,085

Claims	Identification
	<p data-bbox="617 321 1755 354">Android Enterprise Work Profile allows work profile administrator to control the deletion of data.</p> <div data-bbox="814 521 1675 1122" style="border: 2px solid red; padding: 10px;"> <p data-bbox="856 537 1482 565">What policies can my organization manage on my device?</p> <p data-bbox="856 578 1625 716">When you first add a work profile to your device, you need to install a device policy controller app (selected by your organization) as part of the setup process. This app manages your work profile, presents the terms of use, and details the data on your device that is captured and recorded. You must review and accept the user license agreement to set up your work profile.</p> <p data-bbox="856 732 1583 784">If your device is personally-owned, your organization can carry out some or all of the following actions:</p> <ul data-bbox="856 800 1629 1117" style="list-style-type: none"> • Remotely create, access, and <u>delete</u> data in your work profile • Enforce minimum passcode requirements on your work profile and device • Change the password to your managed account (the account associated with your work profile) • Suspend access to your work profile • Restrict what can be shared across your work and personal profiles • Block screen captures in your work profile • Manage access to your organization's corporate mail server and internal data • Remotely install (and uninstall) apps and certificates in your work profile • Manage permissions and other settings for apps in your work profile </div> <p data-bbox="617 1154 1860 1182">https://support.google.com/work/android/answer/7502354?sjid=15190572361787352145-NC#zippy=%2Ci-own-my-device</p>